Antrag 2022/II/Innen/7

Jusos Hamburg

Der/Die Landesparteitag möge beschließen:

Keine Massenüberwachung in einer freien Gesellschaft

Der Landesparteitag der SPD Hamburg möge zur Weiterleitung an den SPD-Bundesparteitag beschließen:

Forderungen:

Die SPD-Fraktionen in den Landesparlamenten und sozialdemokratischen Mitglieder in den Landesregierungen sowie die SPD-Bundestagsfraktion und die sozialdemokratischen Mitglieder der Bundesregierung sind aufgerufen die nachstehenden Positionen umzusetzen.

1.) Alle Länder und der Bund führen Überwachungsgesamtrechnungen in gegenseitiger Berücksichtigung und unter Beachtung europäischer Ermächtigungen durch. Bis zum Abschluss dieses Prozesses werden Sicherheitsbehörden keine neuen Befugnisse eingeräumt und auf europäischer sowie völkerrechtlicher Ebene stimmt die Bundesrepublik Deutschland entsprechenden Rechtsakten oder Maßnahmen nicht zu. Die Überwachungsgesamtrechnung erfolgt jeweils durch ein unabhängiges Gremium und wird regelmäßig, aber spätestens alle drei Jahre, wiederholt. Sie umfasst eine Überprüfung aller Ermächtigungen, den Umfang ihrer Ausübung, ihrer Effektivität, aller anderen vergleichbaren und relevanten Umstände und orientiert sich an wissenschaftlichen Erkenntnissen. Ihre Ergebnisse sind öffentlich. Einzelne Informationen dürfen ausnahmsweise nicht veröffentlicht werden, soweit überragend wichtige Interessen ihre Geheimhaltung gebieten. Für die Ergebnisse und Empfehlungen gilt ein Berücksichtigungsgebot.

2.) Überwachungsmaßnahmen sehen wir nur individualisiert vor. Massenüberwachung - gleichgültig ob bezogen auf Inhalts- oder Verbindungsdaten, ob im Inland oder Ausland - ganzer Netze, Knotenpunkte, Plattformen oder vergleichbarer Bereiche lehnen wir ab. Entsprechende Befugnisse werden abgebaut. Die Bundesrepublik, ihre Behörden und Stellen wirken auf internationaler und europäischer Ebene darauf hin, entsprechende Praktiken zu beenden und stellen Mitwirkungshandlungen ein.

3.) Wir verankern strenge Auskunfts-, Dokumentations- und Löschpflichten für Sicherheitsbehörden. Dabei werden insbesondere schriftliche Begründungspflichten für Abfragen normiert, sowie Löschpflichten verbindlich festgelegt und nicht in das Ermessen der Behörde gestellt. Wir verankern dienst- und strafrechtliche Konsequenzen sollten diese Maßgaben nicht eingehalten werden. Es wird eine unabhängige und vor allem regelmäßige und unangekündigte Kontrolle vorgenommen.

4.) Automatisierte Anwendungen zur Datenverarbeitung und Analyse sind nur ausnahmsweise einzusetzen. Dies gilt insbesondere für von privaten Unternehmen entwickelte Anwendungen, deren Quellcode nicht öffentlich ist. Anwendungen, die eine dafür vorgesehene pluralistisch besetzte staatliche Stelle nicht kontrollieren konnte, dürfen nicht eingesetzt werden. Ein Mensch muss stets die endgültige Entscheidungskompetenz haben.

5.) Wir verankern ein subjektives Recht auf wirksame Verschlüsselungstechnologien ohne staatliche oder sonstige Hintertüren. Maßnahmen, die die Wirksamkeit von Verschlüsselung umgehen oder mittelbar angreifen, wie beispielsweise Client-Side Scanning, lehnen wir ab. Dieses Recht umfasst ausdrücklich auch, soweit technisch möglich, die eigene Wahl der Verschlüsselungstechnologie.

Begründung

Nicht zuletzt durch den Digitalisierungsschub während der Coronapandemie ist die Bedeutung des Internets und online basierter Dienste erneut gewachsen. Insgesamt haben sich in den vergangenen Jahrzehnten zunehmend mehr Bereiche der Gesellschaft und des alltäglichen Lebens digitalisiert. Zeitgleich hat sich auch die Menge an Daten, die wir bei unseren Online-Aktivitäten tagtäglich bewusst und unbewusst produzieren und die tiefe Einblicke in das private Leben liefern können, potenziert.

Spätestens seit den Anschlägen am 11. September 2001 auf das World Trade Center in New York ist dann die Bekämpfung des internationalen Terrorismus in den Mittelpunkt von Debatten um Überwachungsmaßnahmen gerückt. Im Anschluss an verschiedene Anschläge auch in Europa wurden Sicherheitsgesetze wiederholt verschärft. Es wurden Maßnahmen wie die Vorratsdatenspeicherung, die Klarnamenpflicht für Sim-Karten, aber auch die automatisierte Datenverarbeitung im internationalen Flugverkehr eingeführt. Die damit einhergehenden Gefahren oder überhaupt die Zweckmäßigkeit vieler in direkter Reaktion beschlossener Maßnahmen wurden häufig kaum diskutiert. Gesellschaftlich eigentlich unerwünschte Konsequenzen rückten viel mehr erst zeitlich verzögert, im Rahmen von Aufdeckungen wie den Snowden-Leaks, dem Cambridge-Analytica Skandal oder dem jüngsten Datenskandal der Bremer Polizei, zeitweise in den Mittelpunkt.

Vor diesem Hintergrund fehlt es an einer grundsätzlichen sozialdemokratischen und jungsozialistischen Positionierung zum Verhältnis Bürger-Staat im Rahmen der öffentlichen Sicherheit in der digitalisierten Gesellschaft.

Wichtigste Maßgabe muss sein, dass der Zweck nicht die Mittel heiligen kann. Die technischen Möglichkeiten zur digitalen Überwachung sind beinahe umfassend geworden. Um dies festzustellen, bedarf es auch keines Blickes in autoritäre Systeme wie die Volksrepublik China, welche alle Bürger, aber insbesondere ethnische Minderheiten, einer noch vor wenigen Jahren technisch unmöglichen, Massenüberwachung unterzieht. Auch ein Blick in westliche Partnerstaaten wie die USA und Großbritannien zeigt, wie der digitale und öffentliche Raum zunehmend gläsern werden kann.

Eine demokratische Gesellschaft sollte jedoch frei von Massenüberwachung sein. Sie zeichnet sich gerade dadurch aus, dass der Einzelne sich grundsätzlich frei von staatlichem Einfluss entfalten kann. Diese freie Entfaltung ist nicht oder nur eingeschränkt möglich, wenn Menschen befürchten, überwacht zu werden. Gerade die schwere Durchschaubarkeit digitaler Überwachung verstärkt diesen Effekt; sie ist im Einzelnen kaum erkennbar und entzieht sich häufig in ihrer Reichweite dem individuellen Verständnis.

Dabei geht es nicht darum, Sicherheitsbehörden die Möglichkeit zum effektiven Schutz kollektiver und individueller Rechtsgüter zu nehmen. In einem freiheitlich-demokratischen Rechtsstaat sollte aber das Verhalten des Einzelnen Anknüpfungspunkt für Maßnahmen sein. Das massenhafte Scannen von Inhalten oder grundsätzliche Speichern von Verbindungsdaten trifft jedoch alle Menschen.

Wenn Menschen bewusst wird, dass sie überwacht werden, stellen sie nicht nur strafrechtlich sanktioniertes Verhalten ein, sie zensieren sich selbst. So brach beispielsweise die Suche nach Begriffen rund um Themen wie Geheimdienste und Überwachung nach den Enthüllungen durch Edward Snowden ein. Statt sich aktiv mit der Thematik auseinanderzusetzen, vermieden viele Menschen die Suche nach Begriffen im Zusammenhang mit Geheimdiensten und der nationalen Sicherheit, um nicht vermeintlich selbst in den Fokus zu rücken. Entscheidend ist auch nicht, ob Ängste im Einzelnen berechtigt sind, sondern die Auswirkungen eines latenten Gefühls. Solche „chilling effects“ müssen wir vermeiden.

Hinzu kommt, dass bereits der Nutzen von Massenüberwachung mehr als fraglich ist. Die abgefangenen Datenmengen sind häufig zu groß, um sie sinnvoll zu ordnen, entsprechende Maßnahmen sind aufwendig und teuer. Unabhängig von grundsätzlichen grundrechtlichen und ethischen Problemen sind Massenüberwachungsmaßnahmen in der Praxis kaum in der Lage die versprochenen Ergebnisse zu liefern. Selbst interne Untersuchungen der US-Regierung im Anschluss an die Snowden-Enthüllungen, waren nicht fähig konkrete Beispiele für verhinderte Terroranschläge zu nennen. Und auch die EU-Kommission rechnet bei einer Einführung von Maßnahmen wie der sogenannten „Chatkontrolle“ mit einer hohen Anzahl von Falschmeldungen. Auf der Grundlage ihrer Auswirkungen und Ineffizienz lehnen wir sämtliche Massenüberwachungsmaßnahmen, wie beispielsweise die Vorratsdatenspeicherung, aber auch die auf europäischer Ebene vorgeschlagene „Chatkontrolle“, entschieden ab.

Vor diesem Hintergrund gilt es eine Bestandsaufnahme von Befugnissen und Möglichkeiten in gegenseitiger Berücksichtigung durchzuführen. Insbesondere soll die Zusammenarbeit zwischen Sicherheitsbehörden dabei beachtet werden. Die regelmäßige Vornahme umfassender Überwachungsgesamtrechnungen muss gesetzlich vorgeschrieben werden. Dabei geht es nicht nur darum, regelmäßig die Effektivität schwerwiegender Maßnahmen zu überprüfen, sondern auch darum einen Austausch zwischen Sicherheitsbehörden und Zivilgesellschaft zu ermöglichen. Insbesondere die Arbeit von Sicherheitsbehörden muss in einer Demokratie transparent sein, um gegenseitiges Vertrauen wiederherzustellen oder zu stärken.

Um eine effektive Kontrolle zu ermöglichen braucht es ebenfalls umfassende Dokumentations-

und Auskunftspflichten, genau wie definierte Lösch- und Speicherpflichten. Nicht nur die wiederholte Weigerung der Bremer Polizei, Datensätze auch von Zeugen und Opfern zu löschen, oder die nachträgliche legalisierten Europol-Datenbanken haben gezeigt, dass systematische Probleme bei der Gesetzmäßigkeit der Verwaltung und Rechtsdurchsetzung im Rahmen staatlicher Datensammlungen bestehen. Auf der anderen Seite führt mangelnde Kontrolle dazu, dass die Aufklärung der rechtsterroristischen Terroranschläge des NSU und die Rolle deutscher Behörden in diesem Rahmen, durch Löschungen erschwert bis unmöglich gemacht wurden. Auch beim BND hat sich gezeigt, dass mangelnde Dokumentation eine nachträgliche Aufklärung erschwerte, so war kaum noch nachvollziehbar, ob und welche Daten mit internationalen Partnern geteilt wurden.

Im Hinblick auf rechtmäßig gesammelte und gespeicherte Daten, gilt es Gefahren durch automatisierte Datenverarbeitung zu begegnen. Es müssen insbesondere in die Algorithmen eingewobene Diskriminierungen vermieden und einem „automation bias“ vorgebeugt werden. Diese Gefahren werden verstärkt, wenn Anwendungen genutzt werden, deren Funktionsweise weder für Anwender noch für die Menschen deren Daten ausgewertet werden, verständlich ist. Es darf keine „BlackBox Algorithmen“ geben, an deren Ende eine Prognose steht, welche Ausgangspunkt für möglicherweise grundrechtsintensive Maßnahmen ist. Eine alleinige letzte Entscheidungskompetenz eines Menschen zur Absicherung reicht jedoch auf Grund der Gefahren des „automation bias“ nicht aus. Wir fordern deswegen die Nutzung von quelloffenen Anwendungen oder aber zumindest von Anwendungen deren Quellcode vollständig von der jeweiligen Behörde oder einer dafür vorgesehenen Stelle kontrolliert wurden.

Leider ist es zum Schutz der Rechte aller nicht ausreichend, wenn deutsche Behörden und Stellen entsprechende Maßnahmen der Massenüberwachung oder undurchsichtigen Datenverwertung und Analyse unterlassen. Das Internet ist ein globaler Raum mit globalen Akteuren, die häufig schon eigenen Staatsbürgern wenige digitale Rechte zugestehen, aber auf die Rechte fremder Staatsbürger oft keinerlei Rücksicht nehmen. Deutschland ist auf Grund der politischen und wirtschaftlichen Bedeutung oft auch für ausländische Akteure ein relevanter Raum. Auf diese Bedrohung muss der Gesetzgeber reagieren. Es braucht deshalb ein Recht auf effektive Verschlüsselung, ohne jegliche Hintertüren. Zwar ist der Gedanke nachvollziehbar, im Ausnahmefall Kommunikation mitlesen zu wollen. Jedoch gibt es keine Hintertüren „nur für gute Menschen“. Eine Schwächung von Verschlüsselungstechnologien ist immer auch eine Schwächung der Zivilgesellschaft und der eigenen digitalen Sicherheitsstruktur.

Es ist wichtig und richtig, dass unsere Sicherheitsbehörden gegen Bedrohungen vorgehen und individuelle sowie kollektive Rechtsgüter schützen. Dafür brauchen sie die entsprechenden finanziellen und personellen Ressourcen. Wir dürfen aber vor dem Hintergrund wachsender technischer Möglichkeiten auch nicht vergessen, dass nicht alles, was möglich ist, auch gemacht werden sollte. Technologie ist nicht immer die Antwort auf gesellschaftliche Fragen. Grundsätzliche Entscheidungen im Verhältnis Bürger-Staat, wie die freie Entfaltung, sind unbedingt auch in einer digitalisierten Gesellschaft zu erhalten.